# ELECTRONIC MONITORING NOTICE

As required by a New York State law effective in May 2022, the University is obligated to inform its employees that they may be subject to electronic monitoring or recording while using any University-provided equipment or software, as further described below, regardless of whether an employee is working on University property or working remotely. This notice also applies to the use of University-provided systems, applications, and software on a personal device, such as a personal cellular phone or personal computer.

The University has the capability to monitor and retain any electronic mail (email) or transmissions and internet access or usage by an employee on any University-provided equipment, email systems, or software.

The University does not actively monitor electronic mail or transmissions and internet access or usage on any routine basis, but a record of such communications and activity is usually created and may be subject to a search under the circumstances provided in and following the approval process required by the University's Information Technology Policy.

In some instances, voicemail messages are transferred automatically from an employee's University-assigned office telephone to the employee's University-assigned email account and those voicemail files may be accessed under the same circumstances that email is accessed.

Additionally, the University monitors and records employees' telephone conversations or transmissions for the ambulance line and phone lines used for customer service purposes, such as medical appointment phone lines. The University does not record or monitor telephone conversations or transmissions of phone lines not dedicated to emergency calls or customer service purposes. Transmission of voicemail messages to email accounts occurs in some instances as referenced above.

Employees may use a University ID card, University-provided key card or key fob to gain access to University buildings, facilities, or resources. The University logs any University ID card, University-provided key card, or key fob uses or swipes and may review those logs for employment-related purposes. This includes University-provided equipment used to gain access to parking lots requiring permits.

Many areas of the University, including the Medical Center, are subject to video surveillance. This video surveillance captures video only; audio recordings are not captured.

Certain University systems, such as the electronic medical record system used by the University of Rochester Medical Center, create an audit trail to monitor when a record is accessed and by whom. Access and usage of any University systems which allow use or access to Protected Health Information is logged and monitored. Systems which may be actively monitored include eRecord, Epic, and additional programs or software that support clinical care such as laboratory, imaging, and pharmacy.

Personal data, including name and home address, of employees who access URMC electronic medical records may be compared to information related to the accessed record, such as the home address of a patient, to determine if it appears likely the access violated HIPAA and should be investigated further by URMC officials.

The University has the capability to monitor employees' use of University-provided equipment or use of University wireless networks to conduct personal business, such as accessing personal email accounts or personal social media accounts. The University does not routinely, actively monitor such activities, but may do so for the reasons listed in University policy as the basis for searching email.

At all times, the University reserves the right to take such actions as may be necessary to maintain and protect the University's information technology infrastructure and the content of any information in the infrastructure, including email, usage data, and similar information, may be accessed in the course of such maintenance or protection actions.